UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/525,509	03/15/2000	Marcus Peinado	MSFT-0117/147323.1	9495

41505 7590 11/18/2005

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
ONE LIBERTY PLACE - 46TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 11/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/525,509	PEINADO ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-22,25,27-30,33 and 35-37* is/are pending in the application.

4a) Of the above claim(s) *2,23-24, 26, 31-32, 34, and 38-50* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-22,25,27-30,33 and 35-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 26, 2005 has been entered.

2. Claims 1, 3-22, 25, 27-30, 33, and 35-37 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-22, 25, 27-30, 33, and 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over GINTER, Et Al. (US 5,910,987).

As per claim 1:

Ginter, et al. disclose an apparatus for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable and a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request including an old ((n-1)th) key file having the old sets of black box keys, the apparatus comprising: **[COL. 12, lines 7-34]**

a code optimizer/randomizer receiving a master executable and randomized optimization parameters as inputs and producing the (n)the executable as an output; **[COL.117, lines 56-62; COL.118, lines 33-35; and COL.204, lines 1-10]**

a key manager receiving the (n-1)th key file and the (n)th set of black box keys as input **[COL.12, lines 7-15 and COL.118, lines 33-35]**, extracting the old sets of black box keys from the (n-1)th key file **[COL.191, lines 18-66]**, and producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output; **[COL.117, lines 64-67 and COL.118, lines 35-44]**

wherein the (n)th executable and the (n)th key file are to be forwarded to the requesting DRM system **[COL.66, lines 46-64]**,

the key manager producing the (n)th key file encrypted according to a secret **[COL.61, lines 23-43 and COL.66, lines 15-64]**, the apparatus further comprising an injector receiving the (n)th executable from the code optimizer/randomizer as an input **[COL.118, lines 33-35]**, injecting the secret into the (n)th executable in a predetermined location, and producing the injected (n)th executable as an output **[COL.67, lines 55 - COL.68, line 18 and COL.118, lines 35-40]**, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system. **[COL.73, lines 29-67 and COL.74, line 54 - COL.75, line 26]**

Ginter discloses the memory being updateable and Manager 558 making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). Ginter did not exactly claim in terms of extracting old keys but does disclose key storage and retrieving the keys from the key storage areas which is inherently old keys being extracted [COL.117, lines 64-65 and COL.118, lines 37-39]. However, it is obvious to include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified [COL.118, lines 40-44]. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is

obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.

As per claim 2: Cancelled

As per claim 3: Ginter discusses the key manager produces the (n)th key file encrypted according to a symmetric key, the apparatus comprising an injector receiving the (n)th executable from the code optimizer /randomizer as an input, injecting the symmetric key into the (n)th executable in a pre-determined location **[COL.65, lines 22-37 and COL.68, lines 50-63]**, and producing the injected (n)th executable as an output, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system. **[COL.61, lines 23-43 and COL.66, lines 15-64]**

As per claim 4: Ginter discusses the (n)th set of black box keys includes a public - private key pair, and wherein the key manager produces the (n)th key file encrypted according to the private key, the apparatus comprising an injector receiving the (n)th executable from the code optimizer/randomizer as an input, injecting the private key into the (n)th executable in a pre-determined location **[COL.65, lines 22-37 and COL.68, lines 50-63]**, and producing the injected (n)th executable as an output, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system. **[COL.61, lines 23-43 and COL.66, lines 15-64]**

As per claim 5: See COL.67, lines 45-57 and COL.68, lines 50-63; discussing the injector injects the secret into the (n)th executable in the pre-determined location such that the secret is hidden except to the (n)th executable.

As per claim 6: See COL.200, lines 58-63 and COL.203, lines 57-65; discussing the DRM system resides on a computing device has a hardware ID (HWID) associated therewith, wherein the HWID is included in and obtained from the (n-I)th key file, and wherein the injector injects the obtained HWID into the (n)th executable in a pre-determined location.

As per claim 7: See COL.75, lines 16-27 and COL.117, lines 55-62; discussing the code randomizer produces a help file as an output, the help file specifying how the secret is to be injected into the (n)th executable by the injector, and wherein the injector receives the help file as an input and injects the secret into the (n)th executable according to the help file.

As per claim 8: See COL.75, lines 16-27 and COL.117, lines 55-62; discussing the code randomizer produces the help file as an embedded portion of the (n) executable.

As per claim 9: See COL.137, lines 38-45 and COL.139, lines 13-17; discussing a signature generator receiving the (n)th executable as an input, generating a digital signature for the (n)th executable, coupling the generated digital signature to the (n)th executable, and producing the

coupled (n)th executable and digital signature as an output, wherein the coupled (n)th executable and digital signature and the encrypted (n)th key file are to be forwarded to the requesting DRM system.

As per claim 10:

Ginter discloses a method for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable and a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, the request including an old ((n-I)th) key file having the old sets of black box keys, the method comprising: **[COL.6-COL.14]**

receiving a master executable and randomized optimization parameters; **[COL.66, lines 15-32 and COL.117, lines 56-62]**

producing the (n)th executable based on the received master executable and the received randomized optimization parameters and based on a code optimization/randomization technique; **[COL.118, lines 33-35 and COL.204, lines 1-10]**

receiving the (n-1)th key file and the (n)th set of black box keys; **[COL.12, lines 7-15]**

extracting the old sets of black box keys from the (n-1)th key file;

[COL.191, lines 18-66]

producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output based on the extracted old sets of black box keys from the (n-l)th key file and the received (n)th set of black box keys; and **[COL.117, lines 64-67 and 118, lines 35-44]**

forwarding the produced (n)th executable and the produced (n)th key file to the requesting DRM system **[COL.66, lines 46-64],**

wherein producing the (n)th executable comprises producing the (n)th executable with space reserved therein for additional information **[COL.75, lines 16-27 and COL.117, lines 55-62],** to be injected by an injector **[COL.35, line 57 - COL.36, line 36 and COL.75, lines 16-27],** and

wherein producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret, and wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space. **[COL.35, line 57 - COL.36, line 36 and COL.203, lines 57-65]**

Ginter discloses the memory being updateable and Manager making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). Ginter did not exactly claim in terms of extracting old keys but does disclose key storage and retrieving the keys from the key storage areas which is inherently old keys being extracted [COL.117, lines 64-65 and COL.118, lines 37-39]. However, it is obvious to include in

the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified [COL.118, lines 40-44]. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.

As per claim 11: See COL.191, lines 18-66; discussing the old sets of keys in the (n-1)th key file are encrypted according to a secret of an (n-l)th executable, and wherein extracting the old sets of keys comprises obtaining the secret of the (n-1)th executable and applying the secret to the encrypted old sets of keys in the (n-1)th key file.

As per claim 12: See COL.191, lines 18-66; discussing the request includes the (n-1)th executable, wherein the secret is embedded in the (n-1)th executable, and wherein obtaining the secret of the (n-1)th executable comprises extracting the secret from the (n1)th executable.

As per claim 13: See COL.68, lines 50-63 and COL.117, lines 64-67; discussing wherein the secret is maintained in a database, and wherein extracting, the old sets of keys comprises obtaining the secret from the database.

As per claim 14: See COL.191, lines 18-66; discussing the secret is included in the (n-1)th key file, and wherein extracting the old sets of keys comprises obtaining the secret from the (n-1)th key file.

As per claim 15: Ginter discusses the secret is included in the (n-1)th key file encrypted according to a super secret (SUPER(secret)), and wherein extracting the old sets of keys comprises obtaining (SUPER(secret)) from the (n-1)th key file, obtaining the super secret, and applying the super secret to (SUPER(secret)) to obtain the secret. **[COL.191, lines 18-66]**

Ginter discloses the memory being updateable and Manager making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). Ginter did not exactly claim in terms of extracting old keys but does disclose key storage and retrieving the keys from the key storage areas which is inherently old keys being extracted [COL.117, lines 64-65 and COL.118, lines 37-39]. However, it is obvious to include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified [COL.118, lines 40-44]. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.

As per claim 16: See COL.118, lines 30-65 and COL.191, lines 18-66; discussing producing the (n)th key file includes encrypting the (n)th set

of black box keys and the old sets of black box keys according to a secret.

As per claim 17: See COL.118, lines 30-65 and COL.191, lines 18-66; discussing producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret derived from the (n)th set of black box keys.

As per claim 18: See COL.35, line 57 - COL.36, line 36 and COL.192, lines 7-32; discussing producing the (n)th executable comprises embedding the secret therein.

As per claim 19: See COL.68, lines 50-63 and COL.117, lines 64-67; discussing maintaining the secret in a database.

As per claim 20: See COL.35, line 57 - COL.36, line 36 and COL.67, lines 45-45; discussing producing the (n)th key file further includes placing the secret in the (n)th key file.

As per claim 21: Ginter discusses producing the (n)th key file further includes encrypting the secret according to a super secret (SUPER(secret))and placing (SUPER(secret)) in the (n)th key file. **[COL.191, lines 18-66;** Ginter discloses the memory being updateable and Manager making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). Ginter did not exactly claim in terms of extracting old keys but does disclose key storage and retrieving the keys from the key storage areas which is inherently old keys being extracted

[COL.117, lines 64-65 and COL.118, lines 37-39]. However, it is obvious to include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified [COL.118, lines 40-44]. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.]

As per claim 22: See COL.35, line 57 - COL.36, line 36 and COL.203, lines 57-65; discussing the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-1)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the (n-1)th key file, and wherein producing the (n)th key file comprises inserting the extracted HWID into the (n)th key file.

As per claim 23: Cancelled

As per claim 24: Cancelled

As per claim 25: See COL.35, line 57 - COL.36, line 36 and COL.200, lines 58-63 and COL.203, lines 57-65; discussing the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-I)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the

(n-1)th key File, and wherein producing the (n)th executable comprises injecting the extracted HWID into at least a portion of the reserved space.

As per claim 26: Cancelled

As per claim 27: See COL.35, line 57 - COL.36, line 36; COL.67, lines 44-46 and COL.68, lines 50-63; discussing producing the (n)th key file includes encrypting the (n)th set of black box keys and the old sets of black box keys according to a secret, and wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space in a manner hidden except to the (n)th executable.

As per claim 28:

Ginter discusses the method of claim 10 wherein the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the (n-l)th key file further has the HWID therein, wherein the method further comprises extracting the HWID from the (n-l)th key file, and wherein producing the (n)th executable comprises producing the (n)th executable based at least in part on the extracted HWID and based on a code optimization/randomization technique. **[COL.35, line 57 - COL.36, line 36 and COL.203, lines 57-65]**

As per claim 29:

Ginter discloses the method of claim 10 comprising:

receiving, at a code optimizer/randomizer, a master executable and randomized optimization parameters as inputs; **[COL.66, lines 15-32 and COL.117, lines 56-62 and COL.204, lines 1-10]**

producing; at the code optimizer/randomizer, the (n)th executable as an output based on the inputs thereto; receiving, at a key manager, the (n-1)th key file and the (n)th set of black box keys as inputs; **[COL.12, lines 7-15 and COL.118, lines 33-35]**

extracting, at the key manager, the old sets of black box keys from the (n-1)th key file; producing; **[COL.191, lines 18-66]**

at the key manager, the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output **[COL.117, lines 64-67 and 118, lines 35-44]** based on the inputs thereto; and

forwarding the produced (n)th executable and the produced (n)th key file to the requesting DRM system. **[COL.66, lines 46-64]**

As per claim 30:

Ginter discloses the method for producing a new ((n)th) black box for a digital rights management (DRM) system, the (n)th black box for being installed in the DRM system and for performing decryption and encryption functions in the DRM system, the (n)th black box being produced and delivered to the DRM system upon request therefrom and including a new ((n)th) executable, the method comprising:

receiving a master executable and randomized optimization parameters; producing, the (n)th executable based on the received master executable and the received randomized optimization parameters and based on a code optimization/randomization technique; and **[COL.204, lines 1-10]**

forwarding the produced (n)th executable to the requesting DRM system **[COL.66, lines 46-64],**

wherein producing the (n)th executable comprises producing the (n)th executable with space reserved therein for additional information **[COL.75, lines 16-27 and COL.117, lines 55-62],** to be injected by an injector **[COL.35, line 57 - COL.36, line 36 and COL.75, lines 16-27],** and

wherein the (n)th black box further includes a new ((n)th) key file, the (n)th key file having a new ((n)th) set of black box keys and a number of old sets of black box keys, wherein the (n)th key file is produced to include the (n)th set of black box keys and the old sets of black box keys encrypted according to a secret, and wherein producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space. **[COL.35, line 57 - COL.36, line 36; COL.67, lines 44-46 and COL.68, lines 50-63]**

Ginter discloses the memory being updateable and Manager making new keys wherein includes key convolution which is a process that acts on a key and some set of input parameters to yield a new key (col.118, line 37-65). Ginter did not exactly claim in terms of extracting old keys but does disclose key storage and retrieving the keys from the key storage areas which is inherently old keys being extracted [COL.117, lines 64-65 and COL.118, lines 37-39]. However, it is obvious to include in the updating process to include the new set of keys to put in place of the old keys after the old keys have been referenced to and verified [COL.118,

lines 40-44]. Thus, it is obvious for a person of ordinary skill in the art at the time of the invention for Ginter to include the extraction of the old keys from the key file by being able to retrieve specific keys and that it is obvious to have the old keys for verification and referencing purposes in order to produce a new set of black box keys.

As per claim 31: Cancelled

As per claim 32: Cancelled

As per claim 33: See COL.35, line 57 - COL.36, line 36 and COL.200, lines 58-63 and COL.203, lines 57-65; discussing the DRM system resides on a computing device having a hardware ID (HVVID) associated therewith, wherein the request from the DRM system includes the HWID, and wherein producing the (n)th executable comprises injecting the included HWID into at least a portion of the reserved space.

As per claim 34: Cancelled

As per claim 35: See COL.67, lines 45-57 and COL.68, lines 50-63; discussing producing the (n)th executable comprises injecting the secret into at least a portion of the reserved space in a manner hidden except to the (n)th executable.

As per claim 36: See COL.203, lines 57-65; discussing the DRM system resides on a computing device having a hardware ID (HWID) associated therewith, wherein the request from the DRM system includes the HWID, and wherein producing the (n)th executable comprises producing the

(n)th executable based at least in part on the included HWID and based on a code optimization randomization technique.

As per claim 37: See COL.117, lines 64-67 and 118, lines 35-65; discussing receiving, at a code optimizer/randomizer, a master executable and randomized optimization parameters as inputs; and producing, at the code optimizer/randomizer, the (n)th executable as an output based on the inputs thereto.

As per claim 38-50: Cancelled

Response to Arguments

4. Applicant's arguments with respect to claims 1, 10, and 30 have been considered but are moot in view of the new ground(s) of rejection.

The newly amended claims fails to overcome the Ginter, et al. reference because Ginter does teach the limitation of "the key manager producing the (n)th key file encrypted according to a secret [COL.61, lines 23-43 and COL.66, lines 15-64], the apparatus further comprising an injector receiving the (n)th executable from the code optimizer/randomizer as an input [COL.118, lines 33-35], injecting the secret into the (n)th executable in a predetermined location, and

producing the injected (n)th executable as an output [COL.67, lines 55 – COL.68, line 18 and COL.118, lines 35-40], wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system" [COL.73, lines 29-67 and COL.74, line 54 – COL.75, line 26].

A. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., periodically updated**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).**

Applicant's arguments stated that on page 16 of 18, that Ginter reference does not disclose the black box could be periodically updated by obtaining from a centralized black box server a new individualized black box and a corresponding new set of black box keys, as is set forth in claims. However, claim language fails to limit or distinct the limitation of periodically updating. Although, the claimed invention fails to limit the periodically updating and argues there is such, the examiner finds that Ginter does teach retrieving specific keys from the key storage areas and periodically the keys are being updated that are kept in a EEPROM that are secure, updatable, and non-volatile [COL.118, lines 37-44].

Further, Applicant argues that Ginter reference does not at all appreciate that such new set of black box keys should or could be contained in a key file with previous sets of black box keys, as is set forth in claims 1 et seq. so that such previous sets of keys are available for use should the need rise. Ginter does support the limitation "producing the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output", if there is a process of retrieving from the key storage areas in order to update the keys and requests of making new keys [COL.117, lines 64 - COL.118, lines 44]. The examiner finds that the claimed limitation fails to limit applicant's argument of "so that such previous sets of keys are available for use should the need rise". It is obvious the process of retrieving from the key storage is for old keys and if the need arises, the previous sets of keys are used to make new keys as a way of updating.

B. In response to applicant's arguments, the recitation * has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See**

***In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).**

Applicant argues that Ginter does not disclose that a node thereof can or should request a new black box, and thus does not disclose that such a request for an (nth) black box should or could be processed by a code optimizer / randomizer. This limitation is set forth in the preamble and does not give any patentable weight. However, Ginter does include this feature where the Key and Tag Manager supports requests to adjust or make new keys where they are convolute keys that is an algorithmic process that acts on a key and some set of input parameters to yield a new key [COL.118, lines 62-65].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHA

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100